"That One's Gotta Work" Mars Odyssey's use of a Fault Tree Driven Risk Assessment Process[1]

Guy Beutelschies
Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, CA 91109-8099
818-354-2025
guy.beutelschies@jpl.nasa.gov

Abstract—The Odyssey project was the first mission to Mars after the failures of Mars Climate Orbiter and Mars Polar Lander. In addition to incorporating the results of those failure review boards and responding to external "Red Team" reviews, the Odyssey project itself implemented a risk assessment process. This paper describes that process and its use of fault trees as an enabling tool. These trees were used to break the mission down into the functional elements needed to make it a success. By determining how each function could be prevented from executing, a list of failure modes was created. Each fault was individually assessed as to what mitigations could prevent the fault from occurring, as well as what methods should be used to explicitly verify that mitigation. Fault trees turned out to be an extremely useful tool in both identifying risks as well as structuring the development of mitigations.

TABLE OF CONTENTS

1. INTRODUCTION

The Mars Odyssey Project Manager, George Pace, was returning from a business trip about a year before launch. He hailed a cab and, on the way home, the cab driver asked what he did. When he told him that he worked on the next spacecraft going to Mars, the cab driver said "Oh, that one's gotta work!"[1]

In the wake of the Mars Polar Lander and the Mars Climate Orbiter failures, the Mars Odyssey project had to deal with a large increase in risk aversion. NASA headquarters (as well as our nation's cab drivers) recognized that the next spacecraft in the Mars program needed to be a success. In addition to external review boards, the project implemented an internal risk assessment process to identify areas of risk and develop mitigation plans. At the core of this process is the use of fault trees. This paper will describe that process and how fault trees can be effectively used to both identify risks and to structure the development of mitigations.

2. MARS ODYSSEY BACKGROUND

Odyssey Overview

The Mars Odyssey Project was originally called the Mars Surveyor 2001 orbiter. In this paper, the spacecraft is referred to interchangeably as "Odyssey" or "orbiter". Project management is the responsibility of the Jet Propulsion Laboratory (JPL). The spacecraft prime contractor is Lockheed Martin Astronautics (LMA).

This project is part of an ongoing series of unmanned missions to Mars under the Jet Propulsion Laboratory's Mars Exploration Program. The Mars Exploration Program goals include the global observation of Mars to enable understanding of the Mars climatic and geologic history, including the search for liquid water and the evidence of prior or extant life.[2]

Odyssey carries scientific payloads that will determine surface mineralogy and morphology, provide global gamma-ray observations for a full Martian year, and study the Mars radiation environment from orbit. In addition, the orbiter will serve as a data relay for future landers. The orbiter science mission extends for 917 days. During the science mission, the orbiter will also serve as a communications relay for U.S. or international landers in 2003-2004. The orbiter will continue to serve as a telecommunications asset following the science mission; this relay-only phase extends for 457 days, for a total mission duration of 1374 days, or two Mars years. An additional Mars year of relay operations is planned as a goal.[2]

After a 6-month cruise, Odyssey entered a loose elliptical Mars orbit using a bi-propellant main engine burn. It then used a process called aerobraking to achieve its final

[1] 0-7803-6599-2/01/$10.00 © 2001 IEEE

mapping orbit. Aerobraking consists of dipping the spacecraft into the atmosphere on each orbit's periapsis. This lowers the apoapsis, thus turning a highly elliptical orbit into a tight circular mapping orbit.

Science Instruments – The orbiter science payload consists of the Thermal Emission Imaging System (THEMIS), Gamma Ray Spectrometer (GRS), and the Mars Radiation Environment Experiment (MARIE). The GRS instrument suite includes the Gamma Sensor Head (GSH), Neutron Spectrometer (NS), and High Energy Neutron Detector (HEND).[2]

The THEMIS science objectives are to characterize the Martian surface environment by providing high spatial and spectral resolution mineralogical and morphological data by means of visible and infrared imagery.[2]

The experimental objective of the GRS is to determine the elemental composition of the surface of Mars by full planet mapping of elemental abundance with an accuracy of 10% or better and a spatial resolution of about 300 km by remote gamma-ray spectroscopy, and full planet mapping of the hydrogen (with depth of water inferred) and CO_2 abundances by remote neutron spectroscopy.[2]

MARIE science objectives are to characterize specific aspects of the Martian near-space radiation environment, in an attempt to predict anticipated radiation doses to future astronauts and assess its radiobiological effectiveness.[2]

Mission Success Goals – These goals are divided into two categories; primary mission success, which is the absolute minimum that the project must accomplish, and full mission success, which defines the baseline mission that the project is attempting to achieve. These distinctions become important in project resource allocation, design trade studies (especially in the area of fault tolerance) and risk mitigation.

Primary mission success is defined as "Acquire 25% of planned mission data from Mars orbit for two out of three orbiter science instruments (Gamma Ray Spectrometer (GRS), Thermal Emission Imaging System (THEMIS), and the Mars Radiation Environment Experiment (MARIE). Archive the acquired science data in the Planetary Data System."[3]

Full mission success is defined as "Carry out a global survey of Mars from the planned science orbit for one Mars year and collect at least 75% of the planned mission data from the orbiter science instrument complement. Provide communications relay for surface elements from the United States and other spacefaring nations for two Mars years after achieving the science orbit. Archive the acquired science data in the Planetary Data System within six months."[3]

Spacecraft Overview

The spacecraft is three axis stabilized using sun sensors and star cameras for attitude knowledge, an Inertial Measurement unit (IMU) for attitude propagation, and reaction wheels for attitude control. A set of hydrazine thrusters is used for trajectory correction maneuvers as well as for reaction wheel desaturations. A bipropellant main engine is used for orbit insertion. Solar arrays and a nickel hydrogen battery are used to provide power. Telecommunications are provided by an X-Band small deep space transponder over a High Gain antenna (HGA) / Medium Gain Antenna (MGA) assembly. Both the HGA/MGA and the solar array are mounted on their own independent two-axis gimbal systems. The Command and Data handling consist of a RAD6000 processor and a set of interface cards.

The majority of the spacecraft is block redundant with some limited cross strapping.

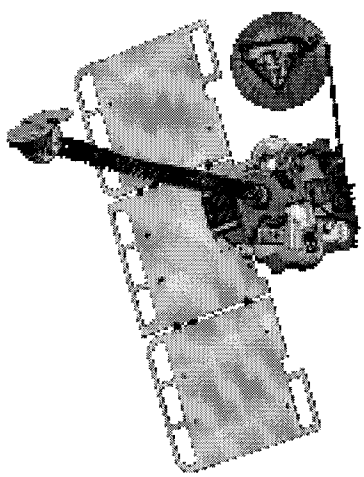


Figure 1 – Odyssey Spacecraft Configuration[2]

Design Paradigm

The approved orbiter design concept was proposed in the spring of 1998 as a build to print version of the Mars Climate Orbiter (MCO). Only mission and payload specific modifications would be made. This assumption allowed an aggressive 36-month development schedule and a relatively low cost. Design inheritance reviews would be conducted, but the assumption was that a successful MCO mission would validate the design. A key thing to keep in mind was that MCO was not scheduled to enter orbit until the fall of 1999, so this was a success oriented assumption.

MSP 98 Failures

On September 23, 1999, MCO fired its main engine to put the spacecraft into Mars orbit. The spacecraft went behind Mars during the burn, as expected. No signal was ever heard from it again. A short time later, the Navigation team determined that the incoming trajectory was much lower than planned, which resulted in the spacecraft entering the atmosphere and presumably burning up.

Failure Descriptions

The failure was traced to an incorrect parameter in the desaturation thrust model used by the Navigation team. This model was provided by the spacecraft team and used English units instead of the specified metric units for the thruster force. This resulted in an incorrect "bias" being used for the forces imparted by the thrusters each time the reaction wheels were desaturated (which averaged roughly once per day). The trajectory the Navigation team assumed the spacecraft was on was therefore different than the actual trajectory.

Failure Review Board Findings

NASA convened three review boards to determine what the failure was and how to prevent future mishaps. There was an internal JPL review board chaired by John Casani, a review board commissioned by the NASA associate administrator for Space Science, chaired by Arthur Stephenson, and a review board commissioned by the NASA administrator, chaired by Tom Young.

Each of the review boards came to the same conclusions as to the cause of the failure. In addition, they each made several broader observations and recommendations for future missions. Those focusing on risk assessment and mitigation are as follows:

The JPL review board[4]:

R11) For each project, assign an experienced person charged with overall mission success oversight during mission operations. This person would ideally have participated in the development project.

R14) The project management training process should be strengthened to emphasize:
- Decision making and evaluating the risk of options
- The importance of identifying mission critical decisions that could be potentially irreversible or catastrophic
- The need for all project-level decisions to be documented, communicated to Project members in a timely fashion, and consistent with project Configuration Management Plan requirements.
- That project-level decision affecting requirements, schedule, resources, and risk should be made with full representation by all project elements with expertise relevant to the decision issue.

R32) Current and future projects must review their operational scenarios and mission timelines for consistency with their Mission Plans and to determine that the necessary planning is in place to support their risk management strategies.

The Arthur Stephenson review board[5]:

MCO Contributing Cause No. 4: Systems Engineering Process
- The lack of an adequate systems engineering function ... resulted in inadequate contingency preparations process to address unpredicted performance during operations, a lack of understanding of several critical operations tradeoffs, and it exacerbated the communications difficulties between the subsystem engineers (e.g. navigations, AACS, propulsion.

MCO Contributing Cause No. 5: Communications Among Project Elements
- Recommendation - ...increase the amount of formal and informal face-to-face communications with all team elements including science, navigation, propulsion, etc. and especially for those elements that have critical interfaces like navigation and spacecraft guidance and control.

MCO Observation No. 2: Independent Reviews
- Recommend ... a formal peer review process on all mission critical events, especially critical navigation events.

MCO Observation No. 3: Contingency Planning process
- Recommend...a systematic assessment of all potential failure modes must be done as a basis for the development of the project contingency plans.

MCO Observation No. 6: Mission Assurance
- Recommend...promote a healthy questioning of "what could go wrong."

MCO Observation No. 8: Navigation Capabilities
- Recommend...personnel should questions and challenge everything – even those things that have always worked.

MCO Observation NO 10: Analyzing What Could Go Wrong
- The Board observed what appeared to be the lack of systematic analyses of "what could go wrong...
- ...the Board observed no fault tree or other a priori analyses of what could go wrong...
- Recommendation: Conduct a fault tree analysis...

The Tom Young review board[6]:

Effective risk identification and management are critical to assure successful deep space missions
- Risk is inherent in deep space missions. Effective identification and management of risk are critical responsibilities of project management and often determine whether a mission will be successful.
- Risk must be assessed and accepted by all accountable parties, including senior management, program management, and project management.

- All projects should utilize established risk management tools such as fault tree analysis and failure effects and criticality analysis.

Frank communication of objectives, requirements, constraints, and risk assessment throughout all phases of the program is critical to successful program/project implementation.

Project Response

It became clear that there were two dominant messages coming out of the MCO review boards:

- Implement a formal process to determine what risks are present so that project management can deal with them.
- Increase project wide communication about how each piece works together to achieve mission success.

Out of NASA headquarters, another message was heard: the next one has to be successful. Two and a half months after the loss of MCO, the Mars Polar Lander, which was the sister craft of MCO, was lost attempting to land on Mars. The failure of two consecutive Mars spacecraft resulted in a shift in paradigms across the Mars program, JPL and Lockheed Martin management, and NASA headquarters. Where the paradigm was once focused on low cost, the new paradigm was focused on risk reduction.

Towards this end, NASA headquarters chartered an independent review of the Odyssey project. These 16 "Red Teams" reviewed every area of the project from spacecraft subsystems, to navigation, to science instruments, to the launch vehicle itself.

In parallel, the Odyssey project decided to implement an internal risk assessment process. While outside review boards are valuable, passing them does not mean the project will succeed. This is born out by the Mars Polar Lander project, which failed after undergoing an intense red team process (albeit after it had already launched), and the Transfer Orbit Stage (TOS) project, which had significant anomalies that were not caught even though it underwent a week long design certification process involving over 100 people for each of its two launches.[7]

The best chance of success comes from the project itself fully understanding its own design and risks. The project manager therefore chartered the author of this paper to implement a risk assessment process for Odyssey.

3. Risk Assessment Process

The risk assessment process was organized into the following steps:

1) Form a team
2) Establish a schedule
3) Perform the assessment
4) Present the results to the project in a peer review forum
5) Repeat steps 3 and 4 for each "round" of risk assessment.
6) Summarize results from all of the risk assessment rounds at a "Project Risk Review"

Team Organization

The key to any successful process is the people involved. In keeping with the goal to have a project risk assessment rather than one just focused on the spacecraft, we formed a combined JPL/LMA team with the lead representatives from each project group:

- Mission Design
- Navigation
- Operations
- Assembly, Test, and Launch Operations (ATLO)
- Spacecraft Systems
- Spacecraft Subsystems
- Payloads

Each one of these teams is crucial to project success, so it was important that the risk assessment process consider them when evaluating what can go wrong.

We knew that leadership was going to be a challenge in making the process work smoothly. Everyone on the project was busy with his or her own tasks, so the lead had to be the engine driving the process. The lead was responsible for scheduling meetings, managing the discussions, and maintaining action item lists to ensure that when "holes" are found, work got done to fill them. To address this, the project manager appointed a senior level systems engineer with experience leading teams.

Senior Level – There was a lot of temptation for team members to work on their own high priority tasks instead of participating fully in the risk assessment process. By assigning a senior engineer, the project made the statement that this was important. The process involved lead individuals from multiple teams so the lead had to have the authority to ensure that the work got assigned and accomplished. In addition, the lead needed to ensure that the outputs of the risk assessment process were fully understood, accepted, and acted upon by the project management.

Systems Orientation – The nature of the process is one of understanding how the different elements of the project work together to achieve the mission success goals. This required a systems mentality as well as sufficient knowledge of each project element to ensure risks were driven out. On Odyssey, we used the lead Spacecraft Systems Engineer, but another option would be to use the Project Systems Engineer.

Team Leadership Skills – The job involved leading a multi-disciplinary team through a process that, by its nature, was very subjective. Since the outcome from this process could result in hardware and software changes, as well as changes in how the mission will be operated, it was critical that the process stayed on schedule and converged on a set of mutually agreed upon risks. Risk areas by their nature were ones where there was uncertainty (otherwise better solutions would already have been chosen). There was, therefore, a strong tendency by talented engineers to want to find solutions before presenting them for the project's consideration. The challenge was knowing when to stop discussion on a specific topic and move on. In addition, there is a certain "art" to making fault trees and a strong personality was needed to ensure that the teams did not waste its time debating aesthetics as opposed to real issues. In summary, team leadership skills were necessary to keep the group on track, on schedule, and moving toward a consensus position.

Process Schedule

After the team was formed, the next step was to prepare a schedule for performing the risk assessment. When to do this process in the project lifecycle is a question that probably does not have one right answer. For Mars Odyssey, the timing of the MCO and MPL losses ended up driving us to doing this after ATLO was underway. This had the advantage of having a mature design to evaluate, which is important to avoid intruding on normal design tradeoffs. The drawback was that changes found by this process were difficult to incorporate since the hardware was already delivered and the software fairly mature. On the whole, having the process a little closer to the Project Critical Design Review (CDR) would have been advantageous. Conducting a formal risk review of this type any earlier than the CDR would have resulted in less value due to the immaturity of the design, although there is value in developing a fault tree analysis early in the project lifecycle to serve as a design evaluation tool.

Another schedule driver was how to divide the project design into "rounds" for assessment. We decided to do it by project phase: Launch, Mars Orbit Insertion (MOI), and Aerobraking. Each of these "critical" events has a recognizable beginning, end, and set of success criteria; thus making it a manageable task for the team to evaluate and for a fault tree to be developed. In addition, we added another risk assessment round for Background (which covered cruise and mapping/relay) to pick up on any items unique for those phases and to ensure that the overall project success goals were being considered.

Process Elements

The process was divided into three parts: design inspection, verification review, and fault tree development.

Design Inspection – The first step was reviewing the design to look for holes. We walked through the requirements first, to ensure that there were no invalid assumptions being used. We walked through the mission and navigation design, the commands and sequences that the operations team was planning on using, and then covered each of the spacecraft functions that occurred during that phase. We specifically focused on "first-time" activities, functions that would be done for the first time in the mission. By presenting the design to the multi-disciplinary group, we found that it inspired a good dialogue, uncovering some areas of inconsistency between the groups. It also gave us a common understanding and vocabulary when it came time to discuss risk areas.

Verification Review – The next area we covered was test and analysis. We wanted to see how the project was nominally ensuring a successful outcome for that mission phase. To keep the task manageable, we focused on those tests and analyses that were unique for that mission phase. We also focused our attention on the individual verification plans for hardware that would only be used in this mission phase, or would be used in a significantly different manner. Examples of verification methods were hardware qualification tests, subsystem performance analysis, and system level testing on the spacecraft. By reviewing each of these areas, we were able to find holes where incorrect assumptions were being used.

Fault Tree Development – The third area we focused on was the development of fault trees for each individual phase we were assessing. This tree was developed early in the process to help us determine what parts of the design inspection and verification to focus on. We started the fault tree development by developing a criteria for what constitutes "success" for a given mission phase. Launch, for instance, was defined as successful if the spacecraft was on the correct trajectory and in a safe, stable configuration (i.e. no immediate actions were necessary to maintain health and safety of the vehicle). If these two conditions were true, then the ground would have plenty of time to respond to any other problems.

Note that the success criteria do not cover success for the entire mission, but only for that particular mission phase. Only by looking at all of the mission fault trees together would you ensure that the overall mission success goals are met. An example of this is that science data return is not listed as a success criterion for the launch fault tree. If you only looked at that tree, you might infer that a fault preventing the return of science data in the mapping phase was not being evaluated by the project. This would not be the case, since those faults are handled in the background (i.e. mapping) fault tree. The reason for this is, again, to keep the task manageable for each risk assessment round.

After the success criteria were established, we then phrased them in a negative manner (i.e. the spacecraft is <u>not</u> in a safe state) and then asked what fault event could cause that to

occur. Further decomposition was then done to determine what sub-events could cause the original event to occur. This decomposition was done down to an appropriate level. Where we stopped, the bottom most fault event (i.e. leaf of the tree) was a fault that we wanted to specifically address. The criteria for "when do you know you've decomposed enough" as well as a discussion on how fault events are identified will be contained in Section 5 of this paper. Appendix A has an example of the Mars Odyssey Launch Fault Tree to provide an illustration of a completed fault tree.

Once the faults were identified, we then assigned unique numbers to them and collected them into a list. The list contained not only the number and fault, but also columns for the following:

Mitigation – How the project was ensuring that the fault did not prevent mission success either by preventing the fault from occurring, or by having a mechanism to respond if the fault should occur. Examples of this were the use of redundancy, analyses showing large performance margins, and inspections to ensure that the defect was not present.

Test Like You Fly (TLYF) – This column detailed how the mitigation would be verified. If the mitigation was an autonomous use of redundancy, then this entry would list the specific test where the fault was simulated and it was demonstrated that the spacecraft would swap to the redundant unit. We decided to format it by answering the questions, "are you testing like you are flying" to ensure that the test realistically simulated the event. The Lockheed Martin institution in particular required a specific list of TLYF exceptions. The fault tree therefore provided an extra benefit of producing input for that list.

Issue – This column contained a yes or no depending on whether the risk assessment group felt that the mitigation and the verification of that mitigation was sufficient. A "no" denoted that there was no issue that the project needed to be aware of. A "yes" meant that we would have to specifically present this topic to the project.

Recommendation/Comment – This was a place where more detail on the issue could be documented.

Peer Reviews – After each round of risk assessment was completed, a peer review was held to present the results to the entire project. Project management then either accepted each individual risk area or provided direction on what additional mitigations should be implemented to reduce or eliminate the risk. We also invited "peers" from outside the project to provide an external check. This ensured that we didn't miss anything as well as provided an expert opinion to project management on how to accommodate the specific risk areas that the team had identified. Request for Actions (RFA) forms were used to document actions brought up during the review. These were included in the risk leader owned action item list to ensure that there was a single list for all of the actions coming out of the risk assessment process. Each risk area was also put into that action item list to provide a mechanism for tracking their resolution and to document how they were resolved.

Project Risk Review – Once all of the risk assessment rounds had been completed, we had a single review to summarize all of the results not only for the project, but also for upper level managers from JPL, Lockheed Martin, and NASA headquarters. Each risk area was again presented along with whether they were accepted or, if mitigated, what the mitigation was and whether any residual risk remained. Status was also provided on all open action items. The mechanism used to document this was a Project Risk List. This list contained all of the accepted risk areas as well as those risk areas that were considered open (i.e., still had unresolved actions). This list was then maintained and presented at each subsequent project review to ensure that the project, institutional managements, and NASA were continually reminded of what risks were being accepted.

4. ODYSSEY RESULTS

Each risk assessment round resulted in a number of requirement errors being identified as well as several holes in the verification program[9][10][11][12]. In addition to those items, the following risk areas were identified along with what the project eventually decided to do about them[8]. Note that some of these were known prior to the risk assessment process, but the process did provide a mechanism for ensuring the project specifically dealt with each one of them.

Launch

L01 – Limited DSN station coverage
Coverage was limited to a single site and had 10-hour gaps during the first couple months after launch due to the escape trajectory needed for this Mars launch opportunity. The Project decided to contract a station in Chile to fill the gaps for the first month of operations.

L02 – Launch window shorter than usual
The window available for meeting all planned mission requirements was shorter than usual. The project added a secondary launch window to the end by relaxing some mission requirements.

L03 –Delay in Initial acquisition
The delay between launch and initial acquisition was longer than usual. The project held a special technical interchange

meeting with the Deep Space Network (DSN) to ensure they were aware of this. We also had the launch vehicle leave its transponder on longer than usual to aid in acquisition.

L04 – Initial Acquisition Telecom Capability
The process identified concerns about the large antenna off-point angles being used during initial acquisition. The project performed a test with the actual flight antenna to verify performance at those angles.

L05 – Failure to Detect Liftoff trigger
Failure of Liftoff break-wire detection would have resulted in never looking for spacecraft separation. The design was changed to decouple those events so as to be tolerant to this failure.

L06 – Launch Reset Impact on Thermal
A processor reset during launch could have resulted in heaters being left in an undesired state. The design was changed to re-command the heater states upon a reset.

Mars Orbit Insertion (MOI)

M01 – MOI Not Single Fault Tolerant
Fault protection was disabled during MOI to avoid inadvertent entries aborting the burn. Failures of certain components will therefore have resulted in an unsuccessful MOI. The project elected to accept this risk.

M02 – Risk of Reset during MOI
A processor reset during MOI would have resulted in the sequence aborting. The design was modified to provide reset protection all the way up to the slew to the MOI attitude. The project elected to accept the risk during the slew and MOI burn.

M03 – Burn to Oxidizer Depletion
Odyssey fired the main engine until the oxidizer was completely depleted. There was a concern that the detection mechanism might not work, resulting in the engine being fired after the depletion had occurred. The results were potentially catastrophic, because the main engine had not been tested for that type of operation. The project performed more analysis on what depletion actually looks like and ended up increasing the monitor's trigger limit.

M04 – Mass Properties Shift
The two fuel tanks are not isolated from each other. There was a concern that propellant could migrate from one to another resulting in a spacecraft center of gravity imbalance. A detailed analysis was done to show that the attitude control system could accommodate a worst-case imbalance.

M05 – "Stuck in the Hook" after TCM 5
A failure mode was identified where the solar array is put in the passive restraint (i.e. the "hook") next to the spacecraft for the contingency Trajectory Correction Maneuver (TCM) number 5 and then is unable to be moved back out. This would result in the solar array not receiving enough power to charge the battery back up for the MOI burn. Since TCM 5 would have occurred at MOI – 6.5 hours, there may not have been enough time for the ground to respond. The project response was to change the pre-MOI attitude to allow sun on the array in the restrained position. This change also allowed the solar array to be placed in the restraint 2 days before MOI and left there, thus simplifying the TCM 5 sequence since it did not need to have any solar array movement commands in it.

M06 – Oxidizer Freezing
The mission plan called for turning off all heaters on the oxidizer side of the propulsion system after MOI since there would be no oxidizer left to freeze. A concern was raised that small amounts of oxidizer could be left in the system, which would be subjected to freeze/thaw cycles possibly rupturing a line. The project decided to leave the oxidizer heaters on for the remainder of the mission.

M07 – Propellant Mixing
During pressurization and the actual burn, the oxidizer and fuel sides of the propulsion system were not isolated from each other. Even though this was for a short duration, there was a concern that fuel and/or oxidizer could migrate up the lines and come into contact with each other resulting in a line rupture (or worst). The project made a hardware change to the already assembled spacecraft to add check valves.

M08 – MOI Communications
The off-point angle of the antenna was very high during MOI. A concern was raised that the link margins for such large off-points might not be sufficient to maintain carrier lock. We therefore performed a test on the flight antenna to confirm its performance.

Aerobraking

A01 – Risk of Dust Storm
The design required that the ground respond within a few hours if a dust storm occurred to prevent the increased atmospheric density from overheating the spacecraft. We lowered the density we were aerobraking at to provide more heating margin. We also arranged to have the Mars Global Surveyor (MGS) spacecraft provide near real-time dust storm monitoring, with our THEMIS instrument available as a backup monitor.

A02 – Endgame
The short orbits at the very end of aerobraking (i.e. endgame) provided very little time to respond to problems and presented our worst power margins of the entire mission. The project decided to implement a strategy of using excess propellant to eliminate endgame orbits using the thrusters. We also changed our fault protection to trigger a maneuver at the next orbital apoapsis. This would move periapsis out of the atmosphere, giving the ground time to respond.

A03 – Vulnerability to Safe Mode Entries
A concern was raised that entries into safe mode just prior to the drag pass might result in entering the atmosphere before safe mode got to an Earth pointed attitude. This could result in a tumble. The solution we implemented was to have safe mode immediately put the solar array in the restraint instead of the having the array fully extended. This configuration is aero-stable in all atmospheric entry orientations.

A04 – Atmospheric Modeling Uncertainty
A concern was raised that the margins used on atmospheric modeling uncertainty may be insufficient. The project brought on additional support to re-look at the MGS aerobraking experience and determine the right margins.

A05 – Star Camera Performance
We found that the drag pass would heat up the star camera beyond its performance limits. We also found that Mars is in the view of the star camera for large portions of the orbit. We responded by changing the aerobraking sequence to slew to the drag attitude a few minutes early (after the vacuum part of the orbit where camera cooled down). This would allow a good attitude for the star camera to get images.

A06 – Safe Mode Aerodynamic Instability
We discovered that being in the safe mode Earth pointed attitude with the solar array fully extended could cause the spacecraft to tumble when it gets to the drag (i.e. atmosphere) part of certain orbits. The response to risk area A03 of putting the solar array in the restraint also solved this problem.

A07 – Aerobraking Safe Mode Power
We determined that the power margin might not be sufficient to support all fault recovery scenarios. We responded by performing an analysis to determine the worst-case recovery timeline. We then ran a power analysis on that scenario to determine what orbital parameters could be supported and what could not. These limits were then passed to the mission design group for their aerobraking design.

A08 – Gas Ingestion
A concern was raised that an imbalance of fuel between the two tanks could cause pressurant gas to be sent down the thruster lines, thus interfering with their operations. We performed an analysis on this and determined that it was only a problem in certain fault cases. Fault protection settings were therefore "loosened" to allow the gas to be expelled through the thrusters before triggering additional hardware swaps.

Background

B01 – SSPA Power Cycles
It was determined that the test program for the Solid State Power Amplifier (SSPA) did not qualify the device for the expected number of power cycles. We therefore changed the test program to increase cycle life testing. We also change the mission operations plan to reduce the number of SSPA power cycles.

B02 – Protection Against Electrical Shorts
Concerns were raised about the software fault protection used to protect against electrical shorts. We found that the hardware protection was sufficient to protect against large current (i.e. "hard" shorts) and the power margins were sufficient for low current shorts. The project decided that the risk of having a short that was below the hardware trip level but large enough to affect the mission was very low and therefore not worth the work to get the software fault protection calibrated to work correctly.

B03 – Mapping Safe Mode
We were worried that the power margins could not support all failure recovery scenarios. We therefore performed an analysis to determine the worst case mapping fault recovery timeline. We then ran a power analysis on this timeline and ended up changing several fault protection parameters to shorten specific recovery timelines.

B04 – Thruster Cold Starts
We found that fault protection "safe mode" would not allow sufficient time to warm up the thruster catbed prior to firing. Thrusters were re-qualified for lower temperature use and more time was added to safe mode for catbed warm up.

5. Fault Tree Mechanics

The purpose of this section is to provide information and advice on how to develop fault trees for a risk assessment process. Since there is a certain "art" to developing fault trees, there really is no one "right" way to do it. The following section merely presents some things we found to be useful in our process.

Fault Tree Organization

One of the items that can cause a lot of discussion at meetings is how the branches and limbs of the tree should be organized. I had the opportunity to attend several of the MPL failure review board meetings, and I was surprised at the amount of time spent arguing over whether certain branches of the fault tree were better documented under this fault event or that. The thing to keep in mind is that the fault tree is a tool for identifying faults. How you get to that fault becomes a little bit irrelevant after it has been identified. The real question to ask is will a change to how the branches are organized lead to uncovering new faults? There is no one "right" fault tree organization. With that being said, we have a couple of suggestions:

Keep focused on the top-level success criteria - It is easy to start straying off into faults that may affect later mission

events, but not the particular one the fault tree is considering.

Have the lead develop the first fault tree draft – The lead can then present it to a group for review and critique. Having one person first lay it out early in the process will go a long way to ensuring a unified and consistent product. Trying to get a committee to develop a tree from scratch will result in too much time spent organizing the tree, and not enough time identifying faults.

How to Identify Fault Events

Identifying fault events is also an important to whether the fault tree performs as a useful tool. There are a couple of things we recommend:

Don't Dive Too Quickly - The most important thing to keep in mind is not diving too deeply into specific faults. A tree is used to stimulate thinking, so at the higher levels the functions should be very broad. This will help ensure that as you work down, you are not missing some faults. If there are more than four or five sub-events assigned to a particular fault event, then intermediate fault events may be needed.

Only Evaluate Single Faults – Our project had a single point failure policy and therefore we did not have to consider multiple independent faults. This simplified our task immensely.

How deep should the tree go

This is also a topic of contention. You could start with a failure of launch and work all the way down to an individual resistor in a piece of electronics. Since there is only a finite amount of time allocated for fault tree development, it is important to limit how deep the fault tree is carried. We found that two things helped us manage this:

Take advantage of other Project Tools - On our project, we had already developed performed Failure Mode, Effects, and Criticality Analysis (FMECA) on each individual piece of hardware. The FMECAs essentially identified all of the failure modes for each "box" on the spacecraft. We therefore reviewed this information and usually stopped the fault tree at the point where the FMECA took over (i.e. box A fails).

Stop when the Mitigations become the Same – At some point, all of the faults below a certain fault event will have the same mitigation. An example of this is the failure of a redundant piece of hardware. No matter how it fails, the spacecraft will detect lack of functionality and swap to the redundant unit. It is therefore of no value to go down any further because the mitigation is already documented for evaluation. You must be careful, though, because it is possible to miss a failure mode that the spacecraft cannot detect. It is a good idea to at least mentally take the tree one step lower to ensure that the spacecraft detection capability is consistent with how the device can fail.

Use of Excel

The tool we used to document the fault trees was Excel, a commonly used software package from Microsoft®. We wanted to first ensure that anyone on the project could easily access the trees. Since everyone already had this software, and was familiar with its use, Excel met this requirement. This software also had capability to maintain internal consistency as well as allow easy navigation through the data.

Fault Tree Organization – Excel had the capability to organize data on multiple pages within the same workbook. This allowed us to take fault events with a lot of sub-events (i.e. branch with a lot of sub-branches and leaves) and put them on their own page. We thus kept each collection of data to a single page that could be printed and discussed. Each page only had one link above to a previous page although it may link to multiple pages below.

Hyperlinks - Excel also had the capability to insert hyperlinks. The viewer could click on an individual fault event and be automatically taken to the page where this event is expanded into sub-events and faults. This was extremely useful for navigating around large fault trees and helped us with our goal of being able to display our tree one page at a time.

Drawing Feature – To ensure clear communication of our ideas, we wanted the tree to look like a classic fault tree. This meant using OR gates and lines pointing to sub-events and faults. Excel had the capability through its drawing feature to support this. Some fault trees developed by other projects have also used AND gates, but, because of our single point failure policy, we did not need them for our application. In cases where we found a possible need for AND gates, we reworded the fault event to make it independent from any other. This kept the tree simple to understand and supported our goal of evaluating one fault at a time.

Cell Links – It was very important to have a list of all of the faults so that we could assign mitigations, tests, etc. Excel had the capability to link cells together so that if one changed, the other automatically did as well. We thus linked the faults and their identification numbers in the tree to the verification list, which was on its own separate page. This went a long way to ensuring internal consistency. Although we did not take advantage of it, it is possible to link identical occurrences of the same fault in the tree together. Since some faults show up in separate parts of the tree, they get assigned different numbers. We could have linked their mitigations and testing entries together so that one change would modify all of the entries and thereby simplify the work. We did not do this because we were not

sure that each instance of the fault would have the same mitigation. In hindsight, the mitigations were usually the same and, with proper vigilance, selective use of this capability would probably have made our jobs easier.

6. CONCLUSIONS

At the time of this writing, Mars Odyssey had launched and was operating successfully. It had not yet accomplished its mission success goals, which is the real test for a risk assessment process. In looking back at the risk assessment process, it did prove extremely valuable in uncovering problems that external review boards would not have caught. This is not to say that external review boards do not have value; they can be extremely useful in providing a different perspective and asking questions that the project may not have thought about. They cannot, however, replace a solid internal risk assessment process.

The strengths of this process include the use of a multi-disciplinary team from across the project and the fact that it was a formal system that required the project to address each risk area. The unique aspect, however, was the use of fault trees as a core tool to structure the risk assessment process and find holes in the design and verification.

For Odyssey, the outcome of this process resulted in numerous changes all across the project:

- Hardware modifications
- Software modifications
- Changes to operational strategies
- Changes to command sequences
- Additional analysis
- Additional testing

The number and breadth of the findings demonstrate the effectiveness of this risk assessment process.

In addition to their value in the risk assessment process, fault trees were also carried for into operations where they were used for contingency plan identification and development. The fault trees were also used to help define risk reduction tests, which were run to find flaws in the operational sequences and the flight software design.

Fault trees are often relegated to post-failure investigations. Odyssey has found them to be a valuable tool during development and operations to catch the failures before they occur.

Acknowledgements – The author would like to thank the following people:

- Charles Whetsel, whose use of fault trees in the Mars Polar Lander red team provided a valuable example of how fault trees could be used.
- Dave Spencer, the Mars Odyssey flight operations manager, who was responsible for the Mission plan which provided the bulk of the background information used in this paper.
- Steve Jolly (LMA Odyssey Risk Manager) and everyone who else was involved in the Mars Odyssey risk assessment process. The process would not have been a success without their hard work.

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

REFERENCES

[1] *Personal conversation with George* Pace, *former manager of the Mars Odyssey project*, January 2001

[2] *Mars Surveyor 2001 Mission Plan*, Revision B, JPL D-1303, August 2000.

[3] *Mars Surveyor 2001 Project Policies*, JPL D-16091, October 2, 2000.

[4] *Report on the Loss of the Mars Climate Orbiter Mission,* JPL Special Review Board, JPL D-18441, November 11, 1999

[5] *Mars Climate Orbiter Mishap Investigation Board Phase I Report,* November 10, 1999

[6] *Mars Program Independent Assessment Team Summary Report, March 14, 2000*

[7] Personal conversation with Bob Berry, former member of the Transfer Orbit Stage (TOS) review board, September 2001

[8] *Mars Surveyor Program 2001, Project Risk Review,* MSP01-00-0381, September 27, 2000

[9] *Mars Surveyor Program 2001, Risk Reduction – Launch,* MSP01-00-0369, June 21, 2000

[10] *Mars Surveyor Program 2001, Orbiter Risk Reduction Peer Review – MOI,* MSP01-00-0241, May 17, 2000

[11] *Mars Surveyor Program 2001, Orbiter Risk Reduction – Aerobraking Peer Review,* MSP01-00-0369, August 17, 2000

[12] *Mars Surveyor Program 2001, Orbiter Risk Reduction – background,* MSP01-00-0369, September 11, 2000

Error! Bookmark not defined. ***is a spacecraft systems engineer working for the Jet Propulsion Laboratory. He has worked on large projects like Galileo and Cassini and smaller***

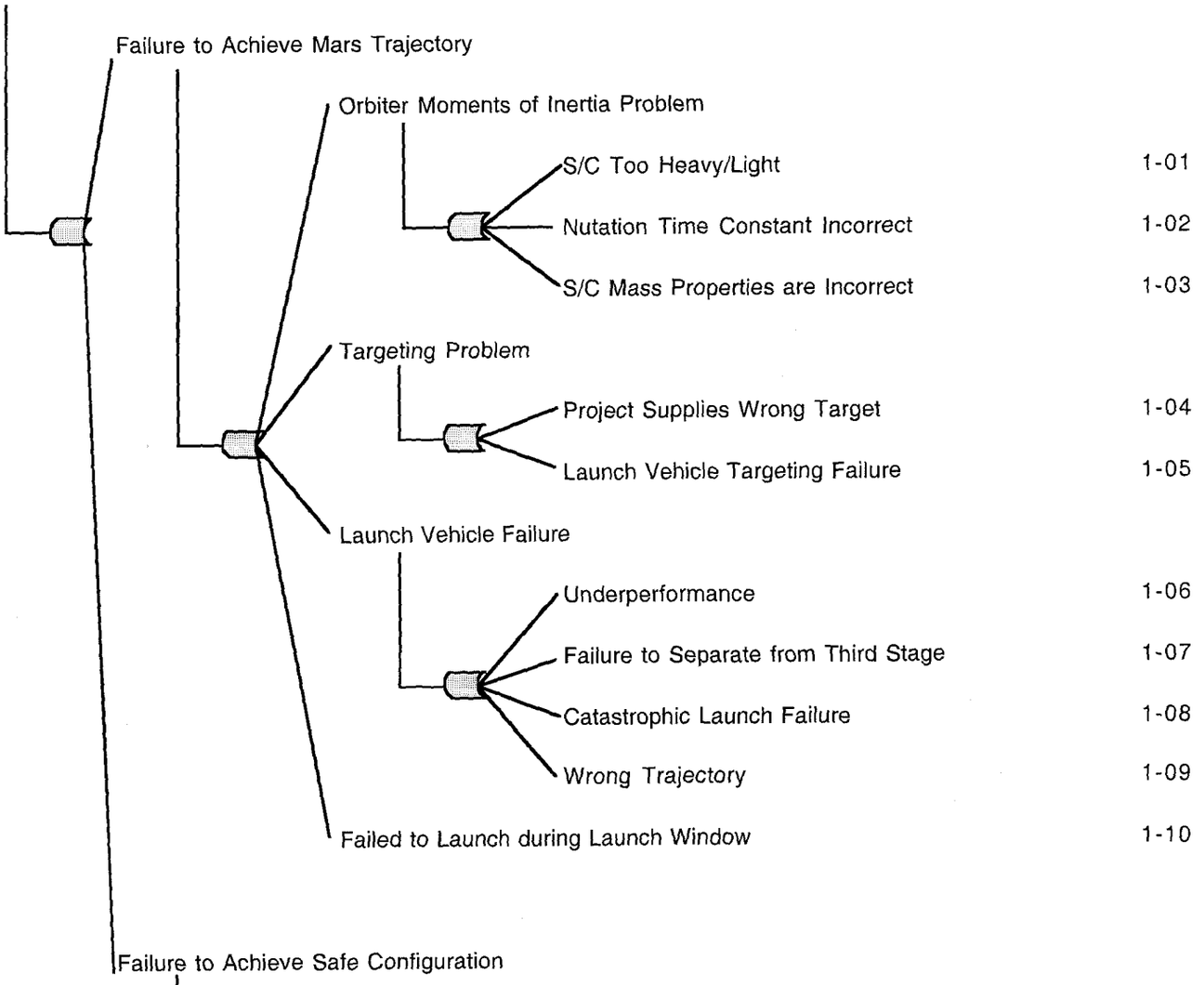
projects like the Mars Pathfinder and the Miniature Systems Technology Integration (MSTI) spacecraft. On Mars Pathfinder he had key roles as a spacecraft system's engineer during development, the electrical test director during testing, and was the flight director during its successful entry and descent to the Martian surface. On Mars Odyssey, he served as the lead spacecraft systems engineer. After launch, he became the Chief Engineer for the operations team. He has a BSAE from the University of Colorado at Boulder, and an MSAE from the University of Southern California.

APPPENDIX A – ODYSSEY LAUNCH FAULT TREE

The following pages contain the launch fault tree used by the Mars Odyssey project. It is included to provide an example of a fault tree actually used by a project in a risk assessment process. Since it is embedded in this document, you will not be able to take advantage of the Excel navigation features (e.g. hyperlinks). Microsoft® Word needs to be set to "Page Layout" in the "View" menu to display the fault tree.

The fault tree version included does not contain references to risk reduction test cases or contingency plans that were added by the operations team.

Launch Failure

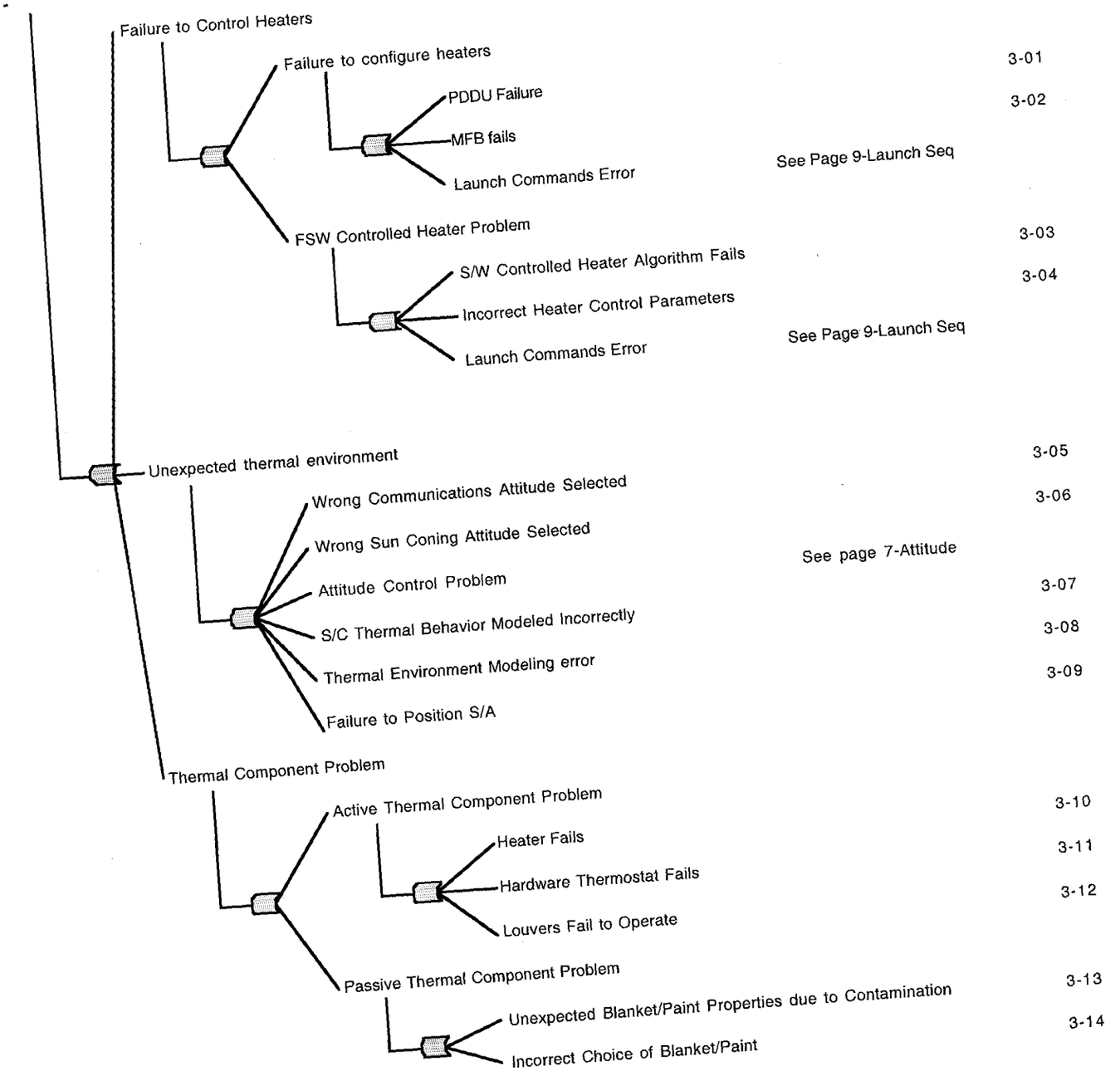


Subpages:

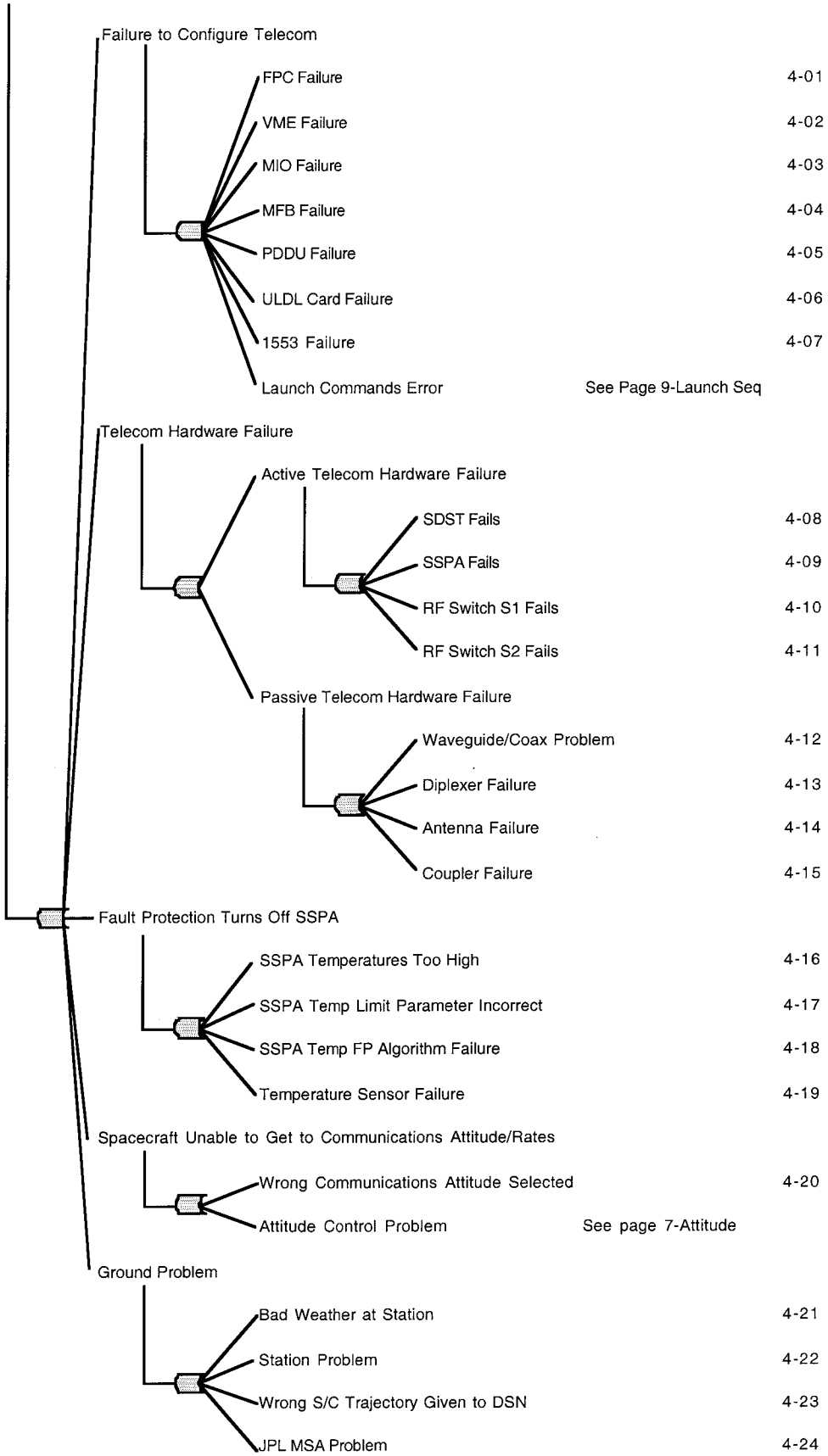
	Attitude	Page 6
	Control Authority Problem	Page 7
	Launch Commands Error	Page 8

Failure to get to Power Stable Configuration

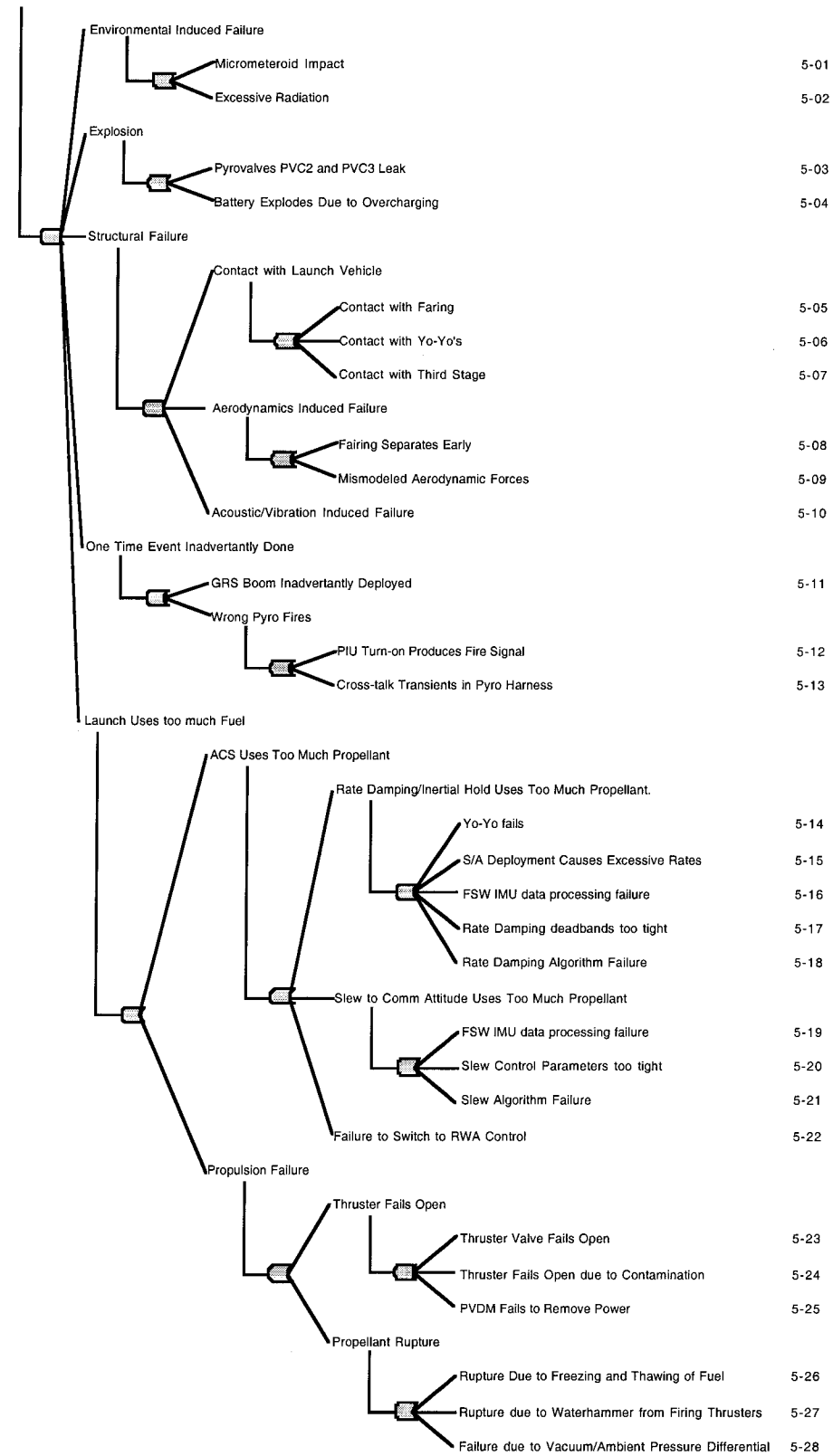
Failure to get to Thermally Stable Configuration

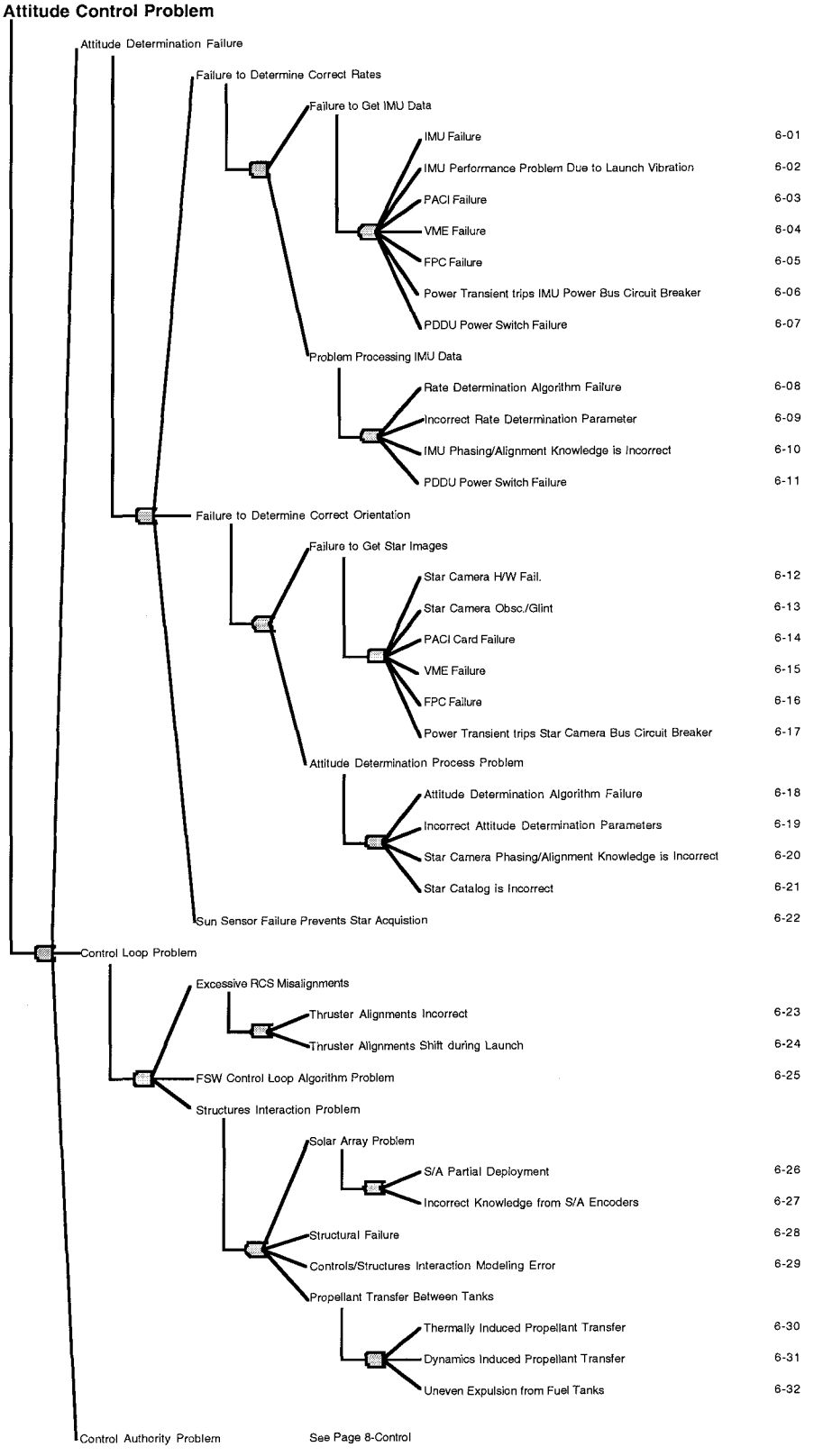


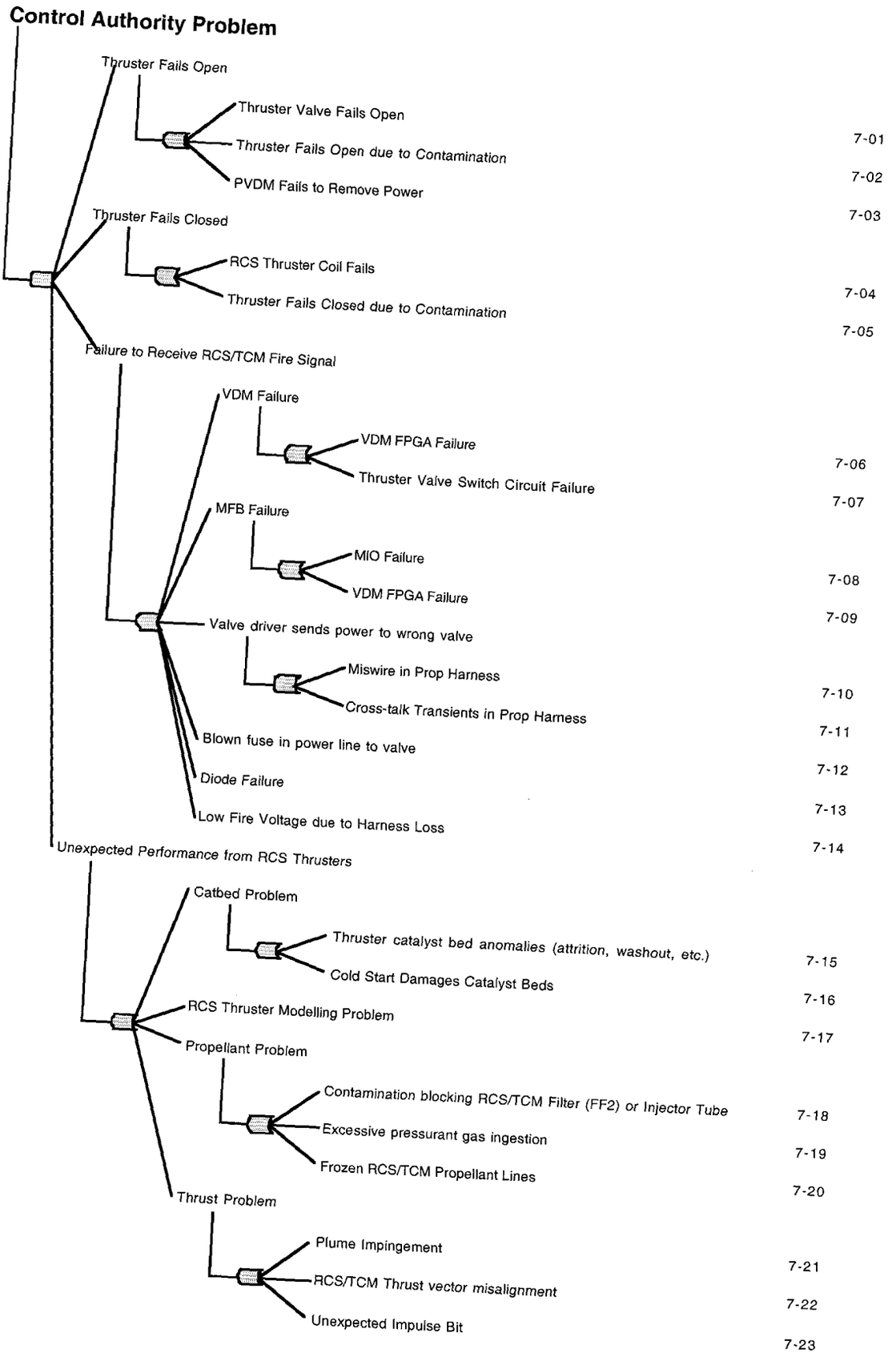
Failure to get to Communications

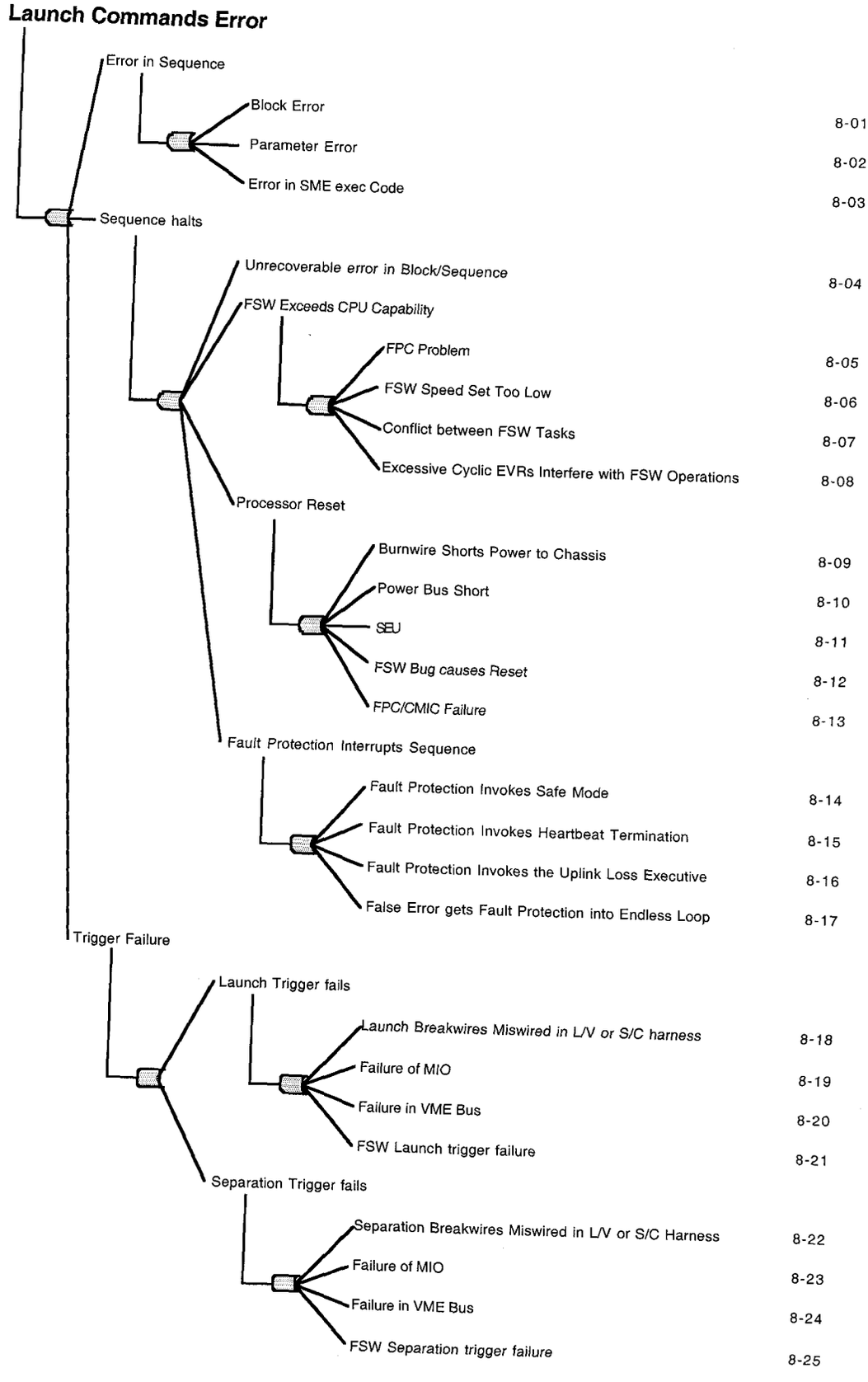


Failure to Continue Mission




Attitude Control Problem
Attitude Determination Failure
Failure to Determine Correct Rates
Failure to Get IMU Data
IMU Failure
6-01
IMU Performance Problem Due to Launch Vibration
6-02
PACI Failure
6-03
VME Failure
6-04
FPC Failure
6-05
Power Transient trips IMU Power Bus Circuit Breaker
6-06
PDDU Power Switch Failure
6-07
Problem Processing IMU Data
Rate Determination Algorithm Failure
6-08
Incorrect Rate Determination Parameter
6-09
IMU Phasing/Alignment Knowledge is Incorrect
6-10
PDDU Power Switch Failure
6-11
Failure to Determine Correct Orientation
Failure to Get Star Images
Star Camera H/W Fail.
6-12
Star Camera Obsc./Glint
6-13
PACI Card Failure
6-14
VME Failure
6-15
FPC Failure
6-16
Power Transient trips Star Camera Bus Circuit Breaker
6-17
Attitude Determination Process Problem
Attitude Determination Algorithm Failure
6-18
Incorrect Attitude Determination Parameters
6-19
Star Camera Phasing/Alignment Knowledge is Incorrect
6-20
Star Catalog is Incorrect
6-21
Sun Sensor Failure Prevents Star Acquistion
6-22
Control Loop Problem
Excessive RCS Misalignments
Thruster Alignments Incorrect
6-23
Thruster Alignments Shift during Launch
6-24
FSW Control Loop Algorithm Problem
6-25
Structures Interaction Problem
Solar Array Problem
S/A Partial Deployment
6-26
Incorrect Knowledge from S/A Encoders
6-27
Structural Failure
6-28
Controls/Structures Interaction Modeling Error
6-29
Propellant Transfer Between Tanks
Thermally Induced Propellant Transfer
6-30
Dynamics Induced Propellant Transfer
6-31
Uneven Expulsion from Fuel Tanks
6-32
Control Authority Problem
See Page 8-Control


Control Authority Problem
Thruster Fails Open
Thruster Valve Fails Open
Thruster Fails Open due to Contamination
PVDM Fails to Remove Power
Thruster Fails Closed
RCS Thruster Coil Fails
Thruster Fails Closed due to Contamination
Failure to Receive RCS/TCM Fire Signal
VDM Failure
VDM FPGA Failure
Thruster Valve Switch Circuit Failure
MFB Failure
MIO Failure
VDM FPGA Failure
Valve driver sends power to wrong valve
Miswire in Prop Harness
Cross-talk Transients in Prop Harness
Blown fuse in power line to valve
Diode Failure
Low Fire Voltage due to Harness Loss
Unexpected Performance from RCS Thrusters
Catbed Problem
Thruster catalyst bed anomalies (attrition, washout, etc.)
Cold Start Damages Catalyst Beds
RCS Thruster Modelling Problem
Propellant Problem
Contamination blocking RCS/TCM Filter (FF2) or Injector Tube
Excessive pressurant gas ingestion
Frozen RCS/TCM Propellant Lines
Thrust Problem
Plume Impingement
RCS/TCM Thrust vector misalignment
Unexpected Impulse Bit
7-01
7-02
7-03
7-04
7-05
7-06
7-07
7-08
7-09
7-10
7-11
7-12
7-13
7-14
7-15
7-16
7-17
7-18
7-19
7-20
7-21
7-22
7-23


Launch Commands Error
Error in Sequence
Block Error
Parameter Error
Error in SME exec Code
Sequence halts
Unrecoverable error in Block/Sequence
FSW Exceeds CPU Capability
FPC Problem
FSW Speed Set Too Low
Conflict between FSW Tasks
Excessive Cyclic EVRs Interfere with FSW Operations
Processor Reset
Burnwire Shorts Power to Chassis
Power Bus Short
SEU
FSW Bug causes Reset
FPC/CMIC Failure
Fault Protection Interrupts Sequence
Fault Protection Invokes Safe Mode
Fault Protection Invokes Heartbeat Termination
Fault Protection Invokes the Uplink Loss Executive
False Error gets Fault Protection into Endless Loop
Trigger Failure
Launch Trigger fails
Launch Breakwires Miswired in L/V or S/C harness
Failure of MIO
Failure in VME Bus
FSW Launch trigger failure
Separation Trigger fails
Separation Breakwires Miswired in L/V or S/C Harness
Failure of MIO
Failure in VME Bus
FSW Separation trigger failure
8-01
8-02
8-03
8-04
8-05
8-06
8-07
8-08
8-09
8-10
8-11
8-12
8-13
8-14
8-15
8-16
8-17
8-18
8-19
8-20
8-21
8-22
8-23
8-24
8-25

Number	Failure Mode	Mitigation Approach	TLYF	Issue?	Recommendation/Comment
1-01	S/C Too Heavy/Light	Spacecraft is wieghed just prior to mating with third stage.	Yes - Measuring system is calibrated.	No	
1-02	Nutation Time Constant Incorrect	Analysis and subscale test data shows that nutation time constant meets requirements.	No - but test is done using subscale tanks.	No	
1-03	S/C Mass Properties are Incorrect	Spacecraft is measured on spin table at KSC.	Yes - Spin table is calibrated.	No	
1-04	Project Supplies Wrong Target	Verified by analysis	No - Done by analysis.	Yes	Need independent analysis.
1-05	Launch Vehicle Targeting Failure	Standard Delta design.	Yes - Delta has 94% success rate.	No	
1-06	Underperformance	Standard Delta design.	Yes - Delta has 94% success rate.	No	
1-07	Failure to Separate from Third Stage	Standard Delta design.	Yes - Delta has 94% success rate.	No	
1-08	Catastrophic Launch Failure	Standard Delta design.	Yes - Delta has 94% success rate.	No	
1-09	Wrong Trajectory	Standard Delta design.	Yes - Delta has 94% success rate.	No	
1-10	Failed to Launch during Launch Window	Multiple launch attempts. Added secondary launch window.	No - Done by analysis.	Yes	Recommend adding capability for 2 launch opportunities per day.
2-01	S/A Deploy Mechanism Failure	Robust Design	Yes - MCO verified design. 01 hardware verified with S/S deployment test and System walkout.	No	
2-02	Separation False Trigger	2 breakwires and backup timer. FSW triggers when 2 out of 3 show separation.	Yes - breakwires will be tested in ATLO. See verification item "Orbiter FP 22.01". The algorithm will be tested in risk reduction testing. See verification item "Orbiter Mission 3.02".	No	
2-03	FSW Pyro Fire Process Failure	Verified by test.	Yes - see verification items "Orbiter EPS 2.09 - 2.24"	No	
2-04	FPC Failure	CMIC will swap to redundant FPC.	Yes - see verification item "Orbiter FP 39.03"	No	
2-05	PIM FPGA Failure	Fault Protection will swap sides if PIM interface error counters exceed preset value.	Yes - see verification item "Orbiter EPS 14.01".	Yes	Error counter values need to be set to ensure S/A deploy pyros are fired.
2-06	Pyro Switch Circuit Failure	Circuits are redundant.	Yes - see verification items "Orbiter EPS 2.09 - 2.24"	No	
2-07	MFB Failure	Fault Protection will swap sides if MFB failure occurs.	Yes - see verification item "Orbiter FP 34.01".	No	
2-08	Miswire Causes Signal to be Sent to Wrong Pyro	Verified by test.	Yes - see verification items "Orbiter EPS 2.09 - 2.24"	No	
2-09	Insufficient Current to Initiators	Verified by test.	Yes - see verification items "Orbiter EPS 2.09 - 2.24"	No	
2-10	Initiator Fails	Redundant initiators.	Yes - see verification items "Orbiter EPS 2.09 - 2.24"	No	
2-11	Pyro Device Failure	Large margins.	Yes - MCO verified design. 01 hardware verified with S/S deployment test.	No	
2-12	S/A only Partially Deployed	Robust Design Margins	Yes - MCO verified design. 01 hardware verified with S/S deployment test.	No	
2-13	S/A too Hot or Cold	Verified by analysis. Large margin on temperatures before performance degrades significantly.	No - Done by analysis.	No	
2-14	String Failures	Large margins. Power analysis assumes one failed string.	No - Done by analysis.	No	
2-15	CCU does not control Solar Array Voltage	Verified by test.	Yes - see verification item "Orbiter EPS 13.01"	No	
2-16	Battery Not Fully Charged Prior to Launch	Battery charge is verified in countdown procedure.	Yes - see verification item "Orbiter Power 8.01"	No	
2-17	Battery Failure During Discharge	Robust Design with large qualification margins.	Yes - see verification items "Orbiter EPS 15.01 - 15.02"	Yes	Accept the risk of an exempted single point failure item.
2-18	Battery Damaged due to Pre-launch Overcharge	Battery is reconditioned during Launch activities.	Yes - see verification item "Orbiter Power 8.01"	No	
2-19	Incorrect load modeling	Verified by test. Power analysis assumes conservative power values.	Yes - see verification items "Orbiter Power 1.01 - 4.03"	No	
2-20	Short on Power Bus	All power electronics are fully redundant. Standard Design Practices for cabling is deemed sufficient; therefore this failure is deemed non-credible and is listed as exception to SPF policy. Non-critical loads are fused/circuit breaker protected.	Yes - ATLO launch SVT is run and power condition is monitored.	Yes	Accept the risk of an exempted single point failure item.
2-21	Power Switch Fails On	Fault protection will turn offending loads' power bus off.	Yes - see verification items "Orbiter FP 37.01 - 37.12".	No	
2-22	Sequence has Incorrect Command	Verified by test.	Yes - see verification items "Orbiter Blocks 1.01 - 1.08"	No	
2-23	Unable to Unrestrain S/A	Fault Protection will sense this condition and slew S/C to compatible attitude.	Yes - see verification item "Orbiter FP 42.30"	Yes	Accept impact of SOST temps going to acceptance limits.
2-24	S/A Gimbal Fails During Articulation	Verified by test.	Yes - see verification item "Orbiter GN&C 15.12"	Yes	Accept the risk of an exempted single point failure item.
2-25	S/A Gimbal Underperformance during Articulation	Fault Protection will keep attempting to move the gimbal until the final position is reached.	Yes - see verification item "Orbiter FP 32.01"	No	
3-01	PDDU Failure	All heaters have redundant strings.	Yes - see verification item "Orbiter EPS 16.01"	No	
3-02	MFB fails	Fault Protection will swap sides if MFB failure occurs.	Yes - see verification item "Orbiter FP 34.01".	No	
3-03	S/W Controlled Heater Algorithm Fails	Verified by test.	Yes - see verification item "Orbiter FP 47.02".	No	
3-04	Incorrect Heater Control Parameters	Verified by test.	Yes - see verification items "Orbiter Therm 8.01 - 8.08"	No	
3-05	Wrong Communications Attitude Selected	Verified by analysis.	Yes - see verification items "Orbiter Therm 5.01 - 5.07"	Yes	Need independent analysis.
3-06	Wrong Sun Coning Attitude Selected	Verified by analysis.	No - Done by analysis.	Yes	Need independent analysis.
3-07	S/C Thermal Behavior Modeled Incorrectly	Verified by test.	Yes - The purpose of the System Thermal Vac test is to validate the thermal models.	No	
3-08	Thermal Environment Modeling error	Verified by analysis.	No - Done by analysis. Thermal Environments similar to MCO.	No	

Number	Failure Mode	Mitigation Approach	TLYF	Issue?	Recommendation/Comment
3-09	Failure to Position S/A	If the S/A is unable to move, fault protection will sense this and put the S/C in a safe position. The effect will be SDST temperatures will approach acceptance limits.	No - the S/A positioning can not be fully tested in 1g. We do, however, test the ability of the gimbal to move to a specified location - see verification item "Orbiter Mission 3.19"	Yes	
3-10	Heater Fails	All heaters have redundant strings.	Yes - see verification item "Orbiter FP 47.02".	No	
3-11	Hardware Thermostat Fails	All heaters have redundant strings.	Yes - see verification item "Orbiter FP 47.03".	No	
3-12	Louvers Fail to Operate	Louvers are oversized so that failure of one louver blade does not cause thermal problem.	No - although louvers are tested (see verification item "Orbiter Therm 9.01".) a failed louver case is only verified by analysis.	No	
3-13	Unexpected Blanket/Paint Properties due to Contamination	Verified by analysis.	No - Done by analysis.	No	
3-14	Incorrect Choice of Blanket/Paint	Verified by analysis.	No - Done by analysis.	No	
4-01	FPC Failure	CMIC will swap to redundant FPC.	Yes - see verification item "Orbiter FP 39.03"	No	
4-02	VME Failure	Fault protection or ground will swap to redundant unit.	Yes - see verification item "Orbiter FP 34.01".	No	
4-03	MIO Failure	Fault protection or ground will swap to redundant unit.	Yes - see verification item "Orbiter FP 34.01".	No	
4-04	MFB Failure	Fault protection or ground will swap to redundant unit.	Yes - see verification item "Orbiter FP 34.01".	No	
4-05	PDDU Failure	Fault protection or ground will swap to redundant unit.	Yes - see verification items "Orbiter FP 19.01 - 20.60".	No	
4-06	ULDL Card Failure	Fault protection or ground will swap to redundant unit.	Yes - see verification items "Orbiter FP 33.01 - 33.03".	No	
4-07	1553 Failure	Fault protection or ground will swap to redundant unit.	Yes - see verification items "Orbiter FP 23.03 - 23.04".	No	
4-08	SDST Fails	Fault protection or ground will swap to redundant unit.	Yes - see verification items "Orbiter FP 23.01 - 23.12"	No	
4-09	SSPA Fails	Fault protection or ground will swap to redundant unit.	Yes - see verification items "Orbiter FP 24.01 - 24.04"	No	
4-10	RF Switch S1 Fails	Switch already in correct position at launch.	Yes - see verification items "Orbiter FP 20.61 - 20.66"	No	
4-11	RF Switch S2 Fails	Switch already in correct position at launch.	Yes - see verification items "Orbiter FP 20.61 - 20.66"	No	
4-12	Waveguide/Coax Problem	Verified by test.	Yes - see verification items "Orbiter FP 20.61 - 20.66"	Yes	Accept the risk of an exempted single point failure item.
4-13	Diplexer Failure	Verified by test.	Yes - see verification items "Orbiter EEIS 1.01 - 2.06".	Yes	Accept the risk of an exempted single point failure item.
4-14	Antenna Failure	Verified by test.	Yes - see verification items "Orbiter Telecom 7.01 - 7.04"	Yes	Accept the risk of an exempted single point failure item.
4-15	Coupler Failure	Verified by test.	Yes - see verification items "Orbiter EEIS 1.01 - 2.06".	Yes	Accept the risk of an exempted single point failure item.
4-16	SSPA Temperatures Too High	Ground commanding can override this fault protection.	Yes - see verification item "Orbiter FP 47.01".	No	
4-17	SSPA Temp Limit Parameter Incorrect	Parameter is verified by thermal vac test. Parameters are also double checked during launch countdown.	Yes - see verification items "Orbiter FP 24.03 - 24.04"	No	
4-18	SSPA Temp FP Algorithm Failure	Ground commanding can override this fault protection.	Yes - see verification items "Orbiter FP 24.03 - 24.04"	No	
4-19	Temperature Sensor Failure	There are multiple temperature sensors used for this monitor. There are also sanity checks on each sensor's data.	Yes - see verification item "Orbiter FP 47.01".	No	
4-20	Wrong Communications Attitude Selected	Verified by analysis.	No - Done by analysis.	Yes	Need independent analysis.
4-21	Bad Weather at Station	Station condition will be part of launch hold criteria.	No	Yes	Launch hold criteria has not yet been documented.
4-22	Station Problem	Station condition will be part of launch hold criteria.	No	Yes	Launch hold criteria has not yet been documented.
4-23	Wrong S/C Trajectory Given to DSN	Verified by analysis.	No - Done by analysis.	Yes	Need independent analysis.
4-24	JPL MSA Problem	JPL MSA condition will be part of launch hold criteria.	Yes - Ops ORTs will verify MSA ability to command and get telemetry. See verification items "Orbiter EEIS 4.01 - 4.03".	Yes	Launch hold criteria has not yet been documented.
5-01	Micrometeroid Impact	Probability of a Micrometeroid hit during Launch is < 0.001%.	No	No	
5-02	Excessive Radiation	Total dose is not a problem since launch is the first activity of the mission.	No	No	
5-03	Pyrovalves PVC2 and PVC3 Leak	Verified by testing.	Yes - Verified by leak testing each pyrovalve at the component level.	No	
5-04	Battery Explodes Due to Overcharging	Verified via test	Yes - ATLO MOI SVT will practice charging an identical battery	No	
5-05	Contact with Faring	Standard Delta design.	Yes - Delta has 94% success rate.	No	
5-06	Contact with Yo-Yo's	Standard Delta design.	Yes - Delta has 94% success rate.	No	
5-07	Contact with Third Stage	Standard Delta design.	Yes - Delta has 94% success rate.	No	
5-08	Fairing Separates Early	Standard Delta design.	Yes - Delta has 94% success rate.	No	
5-09	Mismodeled Aerodynamic Forces	Verified by analysis. Aerodynamic forces are well known from previous Delta launches.	No - Done by analysis.	No	
5-10	Acoustic/Vibration Induced Failure	Verified by testing.	Yes - ATLO acoustics test verified integrity of design. See verification items "Orbiter Stru 6.01 - 6.02".	No	
5-11	GRS Boom Inadvertantly Deployed	Verified by testing.	Yes - ATLO Launch SVT is run and GRS boom condition is monitored. See verification item "Orbiter Stru 2.06".	No	
5-12	PIU Turn-on Produces Fire Signal	Verified by testing.	Yes - ATLO Launch SVT is run and pyro outputs are monitored. See verification items "Orbiter EPS 1.05 - 1.06".	No	
5-13	Cross-talk Transients in Pyro Harness	Verified by testing.	Yes - ATLO Launch SVT is run and pyro outputs are monitored. See verification items "Orbiter EPS 2.01 - 2.64".	No	

Number	Failure Mode	Mitigation Approach	TLYF	Issue?	Recommendation/Comment
5-15	S/A Deployment Causes Excessive Rates	ACS is put into idle mode during deployment. Fault protection will continue to damp rates until we are within limits. Rates are also much less than tipoff.	Yes - see verification item "Orbiter Mission 3.18"	No	
5-16	FSW IMU data processing failure	Verified by testing.	Yes - see verification item "Orbiter FP 34.01"	No	
5-17	Rate Damping deadbands too tight	Verified by analysis.	No - Done by analysis.	No	
5-18	Rate Damping Algorithm Failure	Verified by testing.	Yes - see verification item "Orbiter FP 30.02"	No	
5-19	FSW IMU data processing failure	Verified by testing.	Yes - see verification item "Orbiter FP 34.01"	No	
5-20	Slew Control Parameters too tight	Verified by analysis.	No - Done by analysis.	No	
5-21	Slew Algorithm Failure	Verified by testing.	Yes - see verification item "Orbiter FP 30.02"	No	
5-22	Failure to Switch to RWA Control	Verified by testing.	Yes - see verification item "Orbiter GN&C 15.44".	No	
5-23	Thruster Valve Fails Open	Series redundant solenoid propellant valves are spring loaded to close with removal of valve power.	Yes - Component, subsystem and ATLO REM Functional test verifies that thruster valves will close with power removed.	No	
5-24	Thruster Fails Open due to Contamination	Propellant filters with margin on capacity; high purity hydrazine is sampled and filtered before loading; contamination control procedures during A&T. Component level contamination control. Thruster valves are series redundant.	Yes - filter qualification tests verified capability.	No	
5-25	PVDM Fails to Remove Power	Two series FETs protect valves from continuous current.	Yes - FET functionality verified in PVDM acceptance test.	No	
5-26	Rupture Due to Freezing and Thawing of Fuel	Thermostatically controlled redundant heaters, thermal isolation of lines and MLI featured in the design. Analysis using correlated thermal models.	Yes - ATLO Thermal Vac test verifies temperature margins and heater functionality.	No	
5-27	Rupture due to Waterhammer from Firing Thrusters	Verified by analysis; MSP 98 feed system waterhammer tests	No - Waterhammer effects were determined during MSP 98 Lander testing conducted at EPL (conditions more severe). Did not exactly duplicate flight operation or configuration, but is readily analyzed for the MSP01 configuration.	No	
5-28	Failure due to Vacuum/Ambient Pressure Differential	Verified by test.	No - verified by analysis	No	
6-01	IMU Failure	Fault protection will swap to redundant unit.	Yes - see verification items "Orbiter FP 2.01 - 2.14".	No	
6-02	IMU Performance Problem Due to Launch Vibration	Fault protection will swap to redundant unit.	Yes - Performance is tested in IMU acceptance vibration test. Swap to redundant unit tested as verification items "Orbiter FP 2.01 - 2.14".	No	
6-03	PACI Failure	Fault protection will swap to redundant unit.	Yes - see verification items "Orbiter FP 1.01 - 1.03"	No	
6-04	VME Failure	Fault protection or ground will swap to redundant unit.	Yes - see verification item "Orbiter FP 34.01".	No	
6-05	FPC Failure	CMIC will swap to redundant FPC.	Yes - see verification item "Orbiter FP 39.03"	No	
6-06	Power Transient trips IMU Power Bus Circuit Breaker	Fault protection will swap to redundant unit.	Yes - see verification items "Orbiter FP 37.01 - 37.12"	No	
6-07	PDDU Power Switch Failure	Fault protection will swap to redundant unit.	Yes - see verification items "Orbiter FP 19.01 - 20.60".	No	
6-08	Rate Determination Algorithm Failure	Verified by testing.	Yes - see verification items "Orbiter FP 31.01 - 31.02".	No	
6-09	Incorrect Rate Determination Parameter	Verified by testing.	Yes - see verification items "Orbiter FP 31.01 - 31.02".	No	
6-10	IMU Phasing/Alignment Knowledge is Incorrect	Verified by testing.	Yes - see verification item "Orbiter GN&C 14.01"	No	
6-11	PDDU Power Switch Failure	Fault protection will swap to redundant unit.	Yes - see verification items "Orbiter FP 19.01 - 20.60".	No	
6-12	Star Camera H/W Fail.	Fault protection will swap to redundant unit.	Yes - see verification items for Star Camera in FP.	No	
6-13	Star Camera Obsc./Glint	Fault protection will intiate sun coning.	Yes - see verification item "Orbiter FP 4.11".	No	
6-14	PACI Card Failure	Fault protection will swap to redundant unit.	Yes - see verification items "Orbiter FP 1.01 - 1.03"	No	
6-15	VME Failure	Fault protection or ground will swap to redundant unit.	Yes - see verification item "Orbiter FP 34.01".	No	
6-16	FPC Failure	CMIC will swap to redundant FPC.	Yes - see verification item "Orbiter FP 39.03"	No	
6-17	Power Transient trips Star Camera Bus Circuit Breaker	Fault protection will swap to redundant unit.	Yes - see verification items "Orbiter FP 37.01 - 37.12"	No	
6-18	Attitude Determination Algorithm Failure	Verified by testing.	Yes - see verification item "Orbiter GN&C 15.14"	No	
6-19	Incorrect Attitude Determination Parameters	Verified by testing.	Yes - see verification item "Orbiter GN&C 15.14"	No	
6-20	Star Camera Phasing/Alignment Knowledge is Incorrect	Verified by testing.	Yes - see verification item "Orbiter GN&C 14.02"	No	
6-21	Star Catalog is Incorrect	Checks are done during launch countdown.	No - Done by analysis.	No	
6-22	Sun Sensor Failure Prevents Star Acquistion	Fault protection checks will ensure that no false sun acquisition is seen. Even so, if star camera gets lock, it will override sun sensor data.	Yes - see verification items "Orbiter FP 31.01 - 31.02"	No	
6-23	Thruster Alignments Incorrect	Verified by testing.	Yes - see verification item "Orbiter Stru 4.01"	No	
6-24	Thruster Alignments Shift during Launch	Verified by testing.	Yes - Alignment done pre and post Acoustics test. See verification item "Orbiter Stru 4.01"	No	
6-25	FSW Control Loop Algorithm Problem	Verified by testing.	Yes - see verification item "Orbiter GN&C 15.14"	No	
6-26	S/A Partial Deployment	Large margins.	Yes - MCO verified design. 01 hardware verified with S/S deployment test.	No	
6-27	Incorrect Knowledge from S/A Encoders	Verified by testing.	Yes - see verification items "Orbiter GN&C 15.04 - 15.05 & 15.08 - 15.09"	No	

Number	Failure Mode	Mitigation Approach	TLYF	Issue?	Recommendation/Comment
6-26	Structural Failure	Verified by testing.	Yes - ATLO acoustics test verified integrity of design. See verification items "Orbiter Stru 5.01 - 5.02 & 6.01 - 6.02"	No	
6-29	Controls/Structures Interaction Modeling Error	Spacecraft is measured on spin table at KSC.	Yes - Spin table is calibrated.	No	
6-30	Thermally Induced Propellant Transfer	Fuel tanks have independently FSW controlled heaters. The temperature differential is also controlled by FSW.	Yes - see verification items "Orbiter Therm 8.01 - 8.08"	No	
6-31	Dynamics Induced Propellant Transfer	Verified by analysis	No - verified by analysis	No	
6-32	Uneven Expulsion from Fuel Tanks	Fuel usage during initial acquisition is not enough to cause imbalance affecting aCS.	No - verified by analysis	No	
7-01	Thruster Valve Fails Open	Series redundant solenoid propellant valves are spring loaded to close with removal of valve power.	Yes - Component, subsystem and ATLO REM Functional test verifies that thruster valves will close with power removed.	No	
7-02	Thruster Fails Open due to Contamination	Propellant filters with margin on capacity; high purity hydrazine is sampled and filtered before loading; contamination control procedures during A&T. Component level contamination control. Thruster valves are series redundant.	Yes - filter qualification tests verified capability.	No	
7-03	PVDM Fails to Remove Power	Two series FETs protect valves from continuous current.	Yes - FET functionality verified in PVDM acceptance test.	No	
7-04	RCS Thruster Coil Fails	Initial Acquisition can be accomplished with a failed thruster.	No - but we do test this case in the STL as part of the risk reduction testing. See verificatio item "Orbiter FP 30.02".	No	
7-05	Thruster Fails Closed due to Contamination	Initial Acquisition can be accomplished with a failed thruster.	No - but we do test this case in the STL as part of the risk reduction testing. See verificatio item "Orbiter FP 30.02".	No	
7-06	VDM FPGA Failure	Fault protection will swap to redundant unit.	Yes - see verification item "Orbiter FP 30.02".	No	
7-07	Thruster Valve Switch Circuit Failure	Fault protection will swap to redundant unit.	Yes - see verification item "Orbiter FP 6.01"	No	
7-08	MIG Failure	Fault protection will swap to redundant unit.	Yes - see verification item "Orbiter FP 34.01".	No	
7-09	VDM FPGA Failure	Fault protection will swap to redundant unit.	Yes - see verification item "Orbiter FP 30.02".	No	
7-10	Miswire in Prop Harness	Verified by test.	Yes - see verification item "Orbiter Prop 6.01"	No	
7-11	Cross-talk Transients in Prop Harness	Standard EMI/EMC shielding practices.	Yes - All pyro outputs are monitored via GPCAM during pyro fire tests.	No	
7-12	Blown fuse in power line to valve	Initial Acquisition can be accomplished with a failed thruster.	No - but we do test this case in the STL as part of the risk reduction testing. See verificatio item "Orbiter FP 30.02".	No	
7-13	Diode Failure	Initial Acquisition can be accomplished with a failed thruster.	No - but we do test this case in the STL as part of the risk reduction testing. See verificatio item "Orbiter FP 30.02".	No	
7-14	Low Fire Voltage due to Harness Loss	Initial Acquisition can be accomplished with a failed thruster.	No - but we do test this case in the STL as part of the risk reduction testing. See verification item "Orbiter FP 30.02".	No	
7-15	Thruster catalyst bed anomalies (attrition, washout, etc.)	Verified by test; use of high purity hydrazine; catalyst bed heaters.	Yes - done during thruster qualification and acceptance test.	No	
7-16	Cold Start Damages Catalyst Beds	Redundant heaters are provided; thermal vac test. Analysis of TCM thruster capability shows that greater than 50 starts at 45 deg C are clealy acceptable (less than 1% catalyst loss), based on Thruster Design Criteria (anchored by 5 lbf Bell Aerospace Thruster Testing).	Yes - ATLO Thermal Vac test verifies temperature margins and heater functionality. See verification items "Orbiter Power 5.02, 5.08, 5.11, & 5.17".	No	
7-17	RCS Thruster Modelling Problem	Verified by analysis and test.	No - Although analysis uses data from Thruster Acceptance tests.	No	
7-18	Contamination blocking RCS/TCM Filter (FF2) or Injector Tube	Propellant filters with margin on capacity; high purity hydrazine is sampled and filtered before loading; contamination control procedures during A&T. Component level contamination control.	Yes - filter qualification tests verified capability.	No	
7-19	Excessive pressurant gas ingestion	Barrier internal to tank keeps fuel tank outlet port covered with propellant under conditions of maneuvering and attitude control thruster firings. Vane device in ox tank functions similarly.	No. PMDs are designed and validated by analysis. However, bubble point tests of the capillary screens are performed to ensure that screens will prevent premature ingestion of pressurant.	No	
7-20	Frozen RCS/TCM Propellant Lines	Thermostatically controlled redundant heaters, thermal isolation of lines and MLI featured in the design. Analysis using correlated thermal models.	Yes - ATLO Thermal Vac test verifies temperature margins and heater functionality. See verification items "Orbiter Power 5.35 - 5.36".	No	
7-21	Plume Impingement	RCS thrusters impinge on S/A. GN&C analysis shows small effect on launch performance. Thermal analysis shows plume heating of S/A is enveloped by aerobraking.	No	No	
7-22	RCS/TCM Thrust vector misalignment	Verified by test.	Yes - Pre and post environmental test alignment verfications are made prior to spacecraft pack and ship.	No	
7-23	Unexpected Impulse Bit	Verified by test. A thruster characterization test will also be run in cruise.	Yes - REM acceptance test and qualification test data.	No	
8-01	Block Error	Verified via test.	Yes - Final sequence verified in STL. See verification items "Orbiter Blocks 1.01 - 1.08".	No	
8-02	Parameter Error	Verified via test.	Yes - Final sequence verified in STL. See verification items "Orbiter Blocks 1.01 - 1.08".	No	
8-03	Error in SME exec Code	Verified via test.	Yes - Final sequence verified in STL. See verification item "Orbiter FP 41.01".	No	

Number	Failure Mode	Mitigation Approach	TLYF	Issue?	Recommendation/Comment
8-04	Unrecoverable error in Block/Sequence	Verified via test.	Yes - Final sequence verified in STL. See verification items "Orbiter Blocks 1.01 - 1.08".	No	
8-05	FPC Problem	Fault protection will swap to redundant unit.	Yes - see verification item "Orbiter FP 39.03"	No	
8-06	FSW Speed Set Too Low	Verified via test.	Yes - CPU margin is monitored during MOI SVT and STL tests. See verification items "Orbiter FSW 4.01 - 4.02".	Yes	Recommend switching from 10 Mhz to 20 Mhz.
8-07	Conflict between FSW Tasks	CPU margin and a priority system are used to ensure no conflicts.	Yes - STL provides good environment to test this. Risk Reduction testing will attempt to force conflicts. See verification items "Orbiter FSW 4.01 - 4.02".	No	
8-08	Excessive Cyclic EVRs Interfere with FSW Operations	FSW designed so that excessive EVRs will not interfere with other FSW tasks. Fault Protection will eventually reboot system if this condition occurs.	Yes - CPU margin is monitored during MOI SVT and STL tests. See verification items "Orbiter FSW 4.01 - 4.02".	No	
8-09	Burnwire Shorts Power to Chassis	Design has current limiting to prevent large current returns through structure impacting the rest of the spacecraft. If a reset should occur, FSW will automatically restart initial acquisition process.	Yes - ATLO will tie a pyro directly to chassis and fire it - see verification item "Orbiter EPS 12.01". Reset recovery will be tested as verification item "Orbiter FP 40.01".	No	
8-10	Power Bus Short	All power electronics are fully redundant. Standard Design Practices for cabling is deemed sufficient; therefore this failure is deemed non-credible and is listed as exception to SPF policy. Non-critical loads are fused/circuit breaker protected.	Yes - ATLO Launch SVT is run and power condition is monitored. See verification items "Orbiter EPS 13.01 - 13.02".	Yes	Accept the risk of an exempted single point failure item.
8-11	SEU	SEU Analysis shows <1% probability of SEU during Launch. Fault Protection will restart acquisition process if a reset occurs.	Yes - see verification item "Orbiter FP 40.01"	No	
8-12	FSW Bug causes Reset	Upon reset, the FSW will restart initial acquisition.	Yes - see verification item "Orbiter FP 40.01"	No	
8-13	FPC/CMIC Failure	Fault protection will swap to redundant unit.	Yes - see verification items "Orbiter FP 7.01 - 7.04" and "Orbiter FP 39.03"	No	
8-14	Fault Protection Invokes Safe Mode	Will result in restart of initial acquisition process.	Yes - see verification item "Orbiter Mission 3.26".	No	
8-15	Fault Protection Invokes Heartbeat Termination	Will result in restart of initial acquisition process.	Yes - see verification item "Orbiter Mission 3.27".	No	
8-16	Fault Protection Invokes the Uplink Loss Executive	Will result in restart of initial acquisition process.	Yes - see verification item "Orbiter Mission 3.28".	No	
8-17	False Error gets Fault Protection into Endless Loop	Fault protection has a limit on how many times a side swap can occur.	Yes - see verification item "Orbiter Mission 3.29".	No	
8-18	Launch Breakwires Miswired in L/V or S/C harness	Verified by Boeing test.	No - Boeing harness tested standalone; not used in end to end test with S/C.	Yes	Decouple separation trigger from launch trigger.
8-19	Failure of MIO	There are 2 breakwires. One is on the MIO, the other is on the PACI. Only 1 breakwire (plus the backup timer) are needed.	Yes - see verification item "Orbiter FP 34.01".	No	
8-20	Failure in VME Bus	Fault protection will swap to redundant unit.	Yes - see verification item "Orbiter FP 34.01".	No	
8-21	FSW Launch trigger failure	Verified by test.	Yes - see verification items "Orbiter Mission 3.01" and "Orbiter Mech 3.01"	No	
8-22	Separation Breakwires Miswired in L/V or S/C Harness	Verified by test.	Yes - see verification item "Orbiter Mission 3.01"	No	
8-23	Failure of MIO	There are 2 breakwires. One is on the MIO, the other is on the PACI. Only 1 breakwire (plus the backup timer) are needed.	Yes - see verification item "Orbiter FP 34.01".	No	
8-24	Failure in VME Bus	Fault protection will swap to redundant unit.	Yes - see verification item "Orbiter FP 34.01".	No	
8-25	FSW Separation trigger failure	Verified by test.	Yes - see verification items "Orbiter Mission 3.09" and "Orbiter Mech 3.02"	No	